

SECURE WINDOWS NT INSTALLATION AND CONFIGURATION GUIDE

VERSION 1.2 vs 1.3

The following list contains specific settings which should be configured to bring an NT system to the security level as outlined in guide version 1.3 (assuming the NT system is currently configured as per guide version 1.2). General changes in version 1.3 of the guide are enhancements to the file system and registry sections as well as updated hotfixes in the appendix. The page and step number as listed in version 1.3 are contained in the table below.

PAGE	STEP #	DESCRIPTION
6-7	3	Change Everyone to Authenticated Users
6-9	4	Remove Everyone; Change Domain Users to Authenticated Users
6-10	5	Change Everyone to Authenticated Users
6-11	6	Change Everyone to Authenticated Users
6-12	7	Change Everyone to Authenticated Users
6-13	8	Change Everyone to Authenticated Users
6-13	9	Change Everyone to Authenticated Users
6-14	10	Remove Everyone and Creator Owner
6-14	11	Change Everyone to Authenticated Users
6-15	12	Change Everyone to Authenticated Users
6-16	13	Add rdisk.exe, ntbackup.exe, regedit.exe, regedt32.exe
6-19	17	Check listed files to ensure 128-bit encryption is being used on system
8-3	3	Configure Software\Classes key
8-4	5	Configure Software\Microsoft\Rpc
8-6	8	Change Everyone to Authenticated Users
8-7	10	Add “windows” subkey, change Everyone to Authenticated Users
8-8	12	Add “CachedLogonsCount” key
8-8	13	Add “DeleteRoamingCache” key
8-9	14	Change Everyone to Authenticated Users
8-10	16	Change Everyone to Authenticated Users
8-10	17	Change Everyone to Authenticated Users
8-11	18	Add “AutoShareServer” and “AutoShareWks” subkeys to disable Admin shares
8-12	19	Add “EnableSecuritySignature” for server SMB packet signing
8-12	20	Add “RestrictNullSessAccess” to restrict null sessions
8-13	21	Change REG_SZ to REG_DWORD
8-14	23	Add “EnableSecuritySignature” for workstation SMB packet signing
8-14	24	Add “EnablePlainTextPassword” to disallow clear text password passing
8-17	30	Add “LMCompatibilityLevel” subkey

